

WHAT IS CLAIMED IS:

- 1 1. A method for preventing malicious network attacks said
2 method comprising:
3 receiving a packet from a client computer;
4 determining a number of packets received during a time
5 interval; and
6 rejecting the packet in response to the number of
7 packets exceeding a packet limit.
- 1 2. The method as described in claim 1 wherein the client
2 computer is identified by a source IP address.
- 1 3. The method as described in claim 1 wherein the
2 determining further includes:
3 identifying a client data area based on a source IP
4 address, the client data area including the
5 number of packets received; and
6 incrementing the number of packets received.
- 1 4. The method described in claim 1 further comprising:
2 determining an action from a plurality of actions
3 based on the number of packets received; and
4 executing the action.
- 1 5. The method described in claim 1 further comprising:
2 receiving a socket request from the client computer;
3 determining a number of sockets opened for the client
4 computer;
5 comparing the number of sockets opened to a socket
6 limit; and
7 determining whether to allow a socket request based on
8 the comparison.

1 6. The method described in claim 1 further comprising:
2 creating configuration settings, the configuration
3 settings including the packet limit.

1 7. The method described in claim 6 further comprising:
2 providing a test script, the test script including one
3 or more attack simulations;
4 processing the attack simulations included in the test
5 script;
6 determining whether to change the configuration
7 settings based on the processing; and
8 changing the configuration settings based on the
9 determination.

1 8. An information handling system comprising:
2 one or more processors;
3 a memory accessible by the processors;
4 one or more nonvolatile storage devices accessible by
5 the processors;
6 a network interface for receiving packets from a
7 computer network; and
8 an packet handling tool to manage packets received
9 from the network interface, the packet handling
10 tool including:
11 means for receiving a packet from a client
12 computer through the network interface;
13 means for determining a number of packets
14 received during a time interval; and
15 means for rejecting the packet in response to the
16 number of packets exceeding a packet limit.

09870630-053401

1 9. The information handling system as described in claim
2 8 further comprising:
3 means for identifying the client computer by a source
4 IP address.

1 10. The information handling system as described in claim
2 8 wherein the means for determining further includes:
3 means for identifying a client data area based on a
4 source IP address, the client data area including
5 the number of packets received; and
6 means for incrementing the number of packets received.

1 11. The information handling system as described in claim
2 8 further comprising:
3 means for receiving a socket request from the client
4 computer;
5 means for determining a number of sockets opened for
6 the client computer;
7 means for comparing the number of sockets opened to a
8 socket limit; and
9 means for determining whether to allow a socket
10 request based on the comparison.

1 12. The information handling system as described in claim
2 8 further comprising:
3 means for creating configuration settings, the
4 configuration settings including the packet
5 limit.

1 13. The information handling system as described in claim
2 12 further comprising:
3 means for providing a test script, the test script
4 including one or more attack simulations;

09870610-09101
TOTAL

5 means for processing the attack simulations included
6 in the test script;
7 means for determining whether to change the
8 configuration settings based on the processing;
9 and
10 means for changing the configuration settings based on
11 the determination.

1 14. A computer program product for preventing malicious
2 network attacks, said computer program product
3 comprising:
4 means for receiving a packet from a client computer;
5 means for detecting a number of packets received
6 during a time interval; and
7 means for rejecting the packet in response to
8 detecting that the number of packets exceeds a
9 packet limit.

1 15. The computer program product as described in claim 14
2 wherein the client computer is identified by a source
3 IP address.

1 16. The computer program product as described in claim 14
2 wherein the determining further includes:
3 means for identifying a client data area based on a
4 source IP address, the client data area including
5 the number of packets received; and
6 means for incrementing the number of packets received.

1 17. The computer program product described in claim 14
2 further comprising:

3 means for determining an action from a plurality of
4 actions based on the number of packets received;
5 and
6 means for executing the action.

1 18. The computer program product described in claim 14
2 further comprising:
3 means for receiving a socket request from the client
4 computer;
5 means for determining a number of sockets opened for
6 the client computer;
7 means for comparing the number of sockets opened to a
8 socket limit; and
9 means for determining whether to allow a socket
10 request based on the comparison.

1 19. The computer program product described in claim 14
2 further comprising:
3 means for creating configuration settings, the
4 configuration settings including the packet
5 limit.

1 20. The computer program product described in claim 19
2 further comprising:
3 means for providing a test script, the test script
4 including one or more attack simulations;
5 means for processing the attack simulations included
6 in the test script;
7 means for determining whether to change the
8 configuration settings based on the processing;
9 and
10 means for changing the configuration settings based on
11 the determination.
12

09870640-01302860